UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/524,260	02/11/2005	Feng Bao	P26663	9878

7055	7590	08/24/2006

GREENBLUM & BERNSTEIN, P.L.C.
1950 ROLAND CLARKE PLACE
RESTON, VA 20191

EXAMINER
VU, MICHAEL T

ART UNIT	PAPER NUMBER
2617	

DATE MAILED: 08/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	10/524,260	BAO ET AL.
	Examiner	Art Unit	
	Michael Vu	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

     4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 February 2005* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

     a)☐ All   b)☐ Some * c)☐ None of:

       1.☐ Certified copies of the priority documents have been received.

       2.☐ Certified copies of the priority documents have been received in Application No. _____.

       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/22/2005*.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

1.   The Art Unit location of your application in the USPTO has changed. To aid in

correlating any papers for this application, all further correspondence regarding this

application should be directed to Art Unit 2617.

Information Disclosure Statement

2.   The information disclosure statement (IDS) submitted on 6/22/2005 is in

compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure

statement is being considered by the examiner.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Agrawal (US 2004/0024901) in view of Sandhu (US 2003/0115452).

Regarding **claim 1**, Agrawal teaches a method of generating an authentication

for updating a mobile communications device's location to a second communications

device (Fig.2, Home Network #210, Public Network #230, Foreign Network #240,

Mobile Device #242), the mobile communications device being registered to a proxy

server (Fig. 2, SIP Proxy maintains current location information), the method comprising

the steps of, at the time of performing the location update [0011, 0031, 0063-0064],

But Agrawal does not clearly teach on i. providing a first input from the proxy

server and a second input from the second communications device to a first algorithm to

generate a shared secret, ii. using the shared secret as the authentication when

transmitting the location update to the second communications device.

However, Sandhu, teaches a system for accessing multiple different network, in

which providing a first and second random numbers that shared key to client

authentication [0009, 0027, 0047-0052].

Therefore, it would have been obvious to one of ordinary skill in the art at the

time the invention was made to modify Agrawal, such that providing a first input from the

proxy server and a second input from the second communications device to a first

algorithm to generate a shared secret, using the shared secret as the authentication

when transmitting the location update to the second communications device, to provide

a better technique for protecting resources over the public network, such as a security

key, encrypted and/or decrypted data over the Internet Network.

Regarding **claim 2**, Agrawal/Sandhu teach a method according to claim 1

wherein the first algorithm is a hash function and wherein the hash of the first and

second random numbers is the shared secret [0027] of Sandhu.

Regarding **claim 3**, the combination of Agrawal/Sandhu teach a method

according to claim 1, wherein the mobile communications device has a device address

(Abstract of Agrawal), the address being derived from a second algorithm using a

cryptographic key associated with the mobile device as the input to the algorithm [0027]

of Sandhu.

Regarding **claim 4**, the combination of Agrawal/Sandhu teach a method

according to claim 3, wherein the second algorithm is a hash function and the hash of

the cryptographic key is the device address of the mobile communications device [0009,

0027, 0047-0052] of Sandhu.

Regarding **claim 5**, the combination of Agrawal/Sandhu teach a method

according to claim 4, wherein the mobile communications device provides the device

address and the cryptographic key to the second communications device and wherein

the second communications device verifies the validity of the device address prior to

providing the second input to the first algorithm [0027, 0047-0052].

Regarding **claim 6**, the combination of Agrawal/Sandhu teach a method

according to claim 5, wherein the verification comprises the steps of: performing a hash

of the received cryptographic key to obtain a digest, and comparing the digest of the

hash function with the received address [0004-0009] of Sandhu.

Regarding **claim 7**, the combination of Agrawal/Sandhu teach a method

according to claim 3, wherein the cryptographic key is a public key of an asymmetric

key pair associated with the mobile communications device [0016-0024] of Sandhu.

Regarding **claim 8**, the combination of Agrawal/Sandhu teach a method

according to claim 7, wherein the second communications device sends an encrypted

copy of the second input to the mobile communications device, the encryption being

performed using the public key of the mobile device [0041-0057] of Sandhu.

Regarding **claim 9**, Agrawal/Sandhu teach a method according to claim 1, further comprising the steps of: using the shared secret as an input to a third algorithm, and obtaining an output from the third algorithm as the authentication [0048-0049] of Sandhu.

Regarding **claim 10**, the combination of Agrawal/Sandhu teach a method according to claim 1, wherein the authentication is a hash of the concatenation of the shared secret and the location update message [0011, 0031, 0063-0064] of Agrawal.

Regarding **claim 11**, the combination of Agrawal/Sandhu teach a method according to claim 10, further comprising the step of transmitting the location update message together with the authentication to the second communications device (Fig. 2, [0011, 0031, 0063-0064] of Agrawal.

Regarding **claim 12**, the combination of Agrawal/Sandhu teach a method according to claim 11, further comprising the step of the second communications device computing a hash of the concatenation of the shared secret ([0009, 0027] of Sandhu), and the received location update message for comparison with the received authentication [0063-0064] of Agrawal.

Regarding **claim 13**, the combination of Agrawal/Sandhu teach a method according to claim 12, wherein if the said comparison is the same, the second communications device registers the new location of the mobile communications device and transmits any subsequent messages to the new location [0005, 0029-0030] of Agrawal.

Regarding **claim 14**, Agrawal/Sandhu teach a method according to claim 1,

wherein the first input from the mobile communications device is a random number

[0027] of Sandhu.

Regarding **claim 15**, Agrawal/Sandhu teach a method according to claim 1,

wherein the second input from the second communications device is a random number

[0027] of Sandhu.

Regarding **claim 16**, the combination of Agrawal/Sandhu teach a method

according to claim 1, wherein the second communications device is mobile (Fig. 2,

Mobile Device #242) of Agrawal, and (Fig. 3, User Device) of Sandhu.

Regarding **claim 17**, Agrawal/Sandhu teach a method according to claim 1,

wherein the second communications device has a fixed inter-network address (Fig. 20

of Agrawal.

Conclusion

5.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Michael Vu whose telephone number is (571) 272-8131.

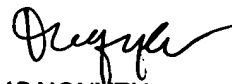The examiner can normally be reached on 8:00am - 6:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Duc Nguyen can be reached on 571-272-7503. The fax phone number for

the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the .

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Michael Vu

DUC NGUYEN
PRIMARY EXAMINER